

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[NORTH DAKOTA](#)

[REGIONAL](#)

[NATIONAL](#)

[INTERNATIONAL](#)

[BANKING AND FINANCE
INDUSTRY](#)

[CHEMICAL AND HAZARDOUS
MATERIALS SECTOR](#)

[COMMERCIAL FACILITIES](#)

[COMMUNICATIONS SECTOR](#)

[CRITICAL MANUFACTURING](#)

[DEFENSE INDUSTRIAL BASE
SECTOR](#)

[EMERGENCY SERVICES](#)

[ENERGY](#)

[FOOD AND AGRICULTURE](#)

[GOVERNMENT SECTOR
\(INCLUDING SCHOOLS AND
UNIVERSITIES\)](#)

[INFORMATION TECHNOLOGY
AND TELECOMMUNICATIONS](#)

[NATIONAL MONUMENTS AND
ICONS](#)

[POSTAL AND SHIPPING](#)

[PUBLIC HEALTH](#)

[TRANSPORTATION](#)

[WATER AND DAMS](#)

[NORTH DAKOTA HOMELAND
SECURITY CONTACTS](#)

UNCLASSIFIED

NORTH DAKOTA

Corps looks to improve Williston levees. The U.S. Army Corps of Engineers is planning a \$20 million upgrade for improving the 50-year old Williston, North Dakota levee system this summer. They are starting with upgrading 16 pressure relief wells, which are 70 to 100 feet deep and relieve pressure. "The levee system functioned very well during this last event, however the levee system is aging and we just need to upgrade," said a Corps official. The Corps is also resurfacing the levee and adding more soil to improve the slope. This work will be done for all 9.2 miles of the levee system. The bulk of the project will take place from Mid-May through the fall. At that time the Corps is requesting the public not use the levee system.

Source: http://www.kfyrtv.com/News_Stories.asp?news=55837

OSHA cites Powers Lake well. The U.S. Office of Safety and Health Administration (OSHA) cited an oil well in Powers Lake, North Dakota, for violations for exposing workers to unsafe conditions, KFJR 5 Bismarck reported March 13. The OSHA inspected Carlson Well Services after an explosion killed two workers and seriously injured two others in September 2011. Violations include failing to ensure an alternate escape on land rigs, failing to properly install a blow-out preventer, and failing to provide protective equipment and clothing. Carlson Well Service is penalized with violations totaling \$85,000. Source:

http://www.kfyrtv.com/News_Stories.asp?news=55754

REGIONAL

(Minnesota) Area fire departments continue to battle fire at Moorhead packaging plant.

Multiple departments continued to battle a fire at the Pactiv Plant in Moorhead, Minnesota, March 14. Damage estimates were in the millions. Crews battled the fire for at least 7 hours. The building was feared to be a total loss as officials said much of the ceiling caved in and the foundation was cracking. Officials evacuated all 45 employees before crews arrived. The 130,000 square-foot plant specialized in making egg cartons by using recycled newspaper and a natural gas oven. "A lot of gas and heat in those ovens, so when they ignite all the lint and the paper lint at the ceiling level can ignite," the Moorhead fire chief said. Moorhead fire officials believed the fire started at the west end of the building at the pulp dryer. Multiple crews were on scene throughout the night giving aid, from Barnesville, Fargo, Dilworth, Glyndon, and Sabin.

Source: <http://www.wday.com/event/article/id/60603/>

(Montana) Florence-Carlton school district closed due to gastroenteritis outbreak. Florence-Carlton school administrators shut down all three schools in Florence, Montana, for the rest of the week after about 110 students called in sick March 15. The superintendent said several students went home sick March 14, but more than 10 percent of the student body was sick March 15. Parents were called shortly before noon March 15 to pick up students. The Ravalli County public health director said the health department planned to conduct a communicable disease investigation after students became ill with acute gastroenteritis. The superintendent said health officials instructed him to shut down the elementary school, middle school, and high school, and all school-related activities for the rest of the week. Classes were scheduled to

UNCLASSIFIED

resume March 19. Source:

<http://www.therepublic.com/view/story/4dbafe6e1bcf4dd8be18fec5f6fde631/MT--Schools-Close-Illness/>

(Montana) 11 firefighters on scene at Bear Trap blaze near Ennis. An abandoned campfire is to blame for a wind-driven wildfire that scorched at least 100 acres of land along the Bear Trap National Recreation Trail, north of Ennis, Montana, the weekend of March 10. As of March 11, 11 firefighters with the Forest Service remained on the scene putting out hot spots, a Forest Service spokeswoman said. Authorities evacuated an estimated 100 people who were recreating there when the fire broke out, she said. Access to the Bear Trap National Recreation Trail, which winds through the Lee Metcalf Wilderness, was closed until further notice. The spokeswoman said crews were expected to be working at the fire for a couple of days. Firefighters from the Bureau of Land Management, Madison County, Montana Department of Fish, Wildlife, and Parks, and the Ennis Volunteer Fire Department assisted the Forest Service in the management of the fire. Source: http://billingsgazette.com/news/state-and-regional/montana/firefighters-on-scene-at-bear-trap-blaze-near-ennis/article_3395c53d-7b6c-5ad4-8e0a-93413eeac311.html

(Wyoming; South Dakota) Keyhole Reservoir high; Belle Fourche near full. Dry weather conditions sparking fires and a Butte County, South Dakota burn ban have not cut rising water in Bureau of Reclamation reservoirs, including Keyhole in northeast Wyoming and the Belle Fourche Reservoir at Orman Dam in Butte County. A Reclamation news release March 12 reported warm weather caused Keyhole Reservoir to rise over a foot in elevation in the last 5 days bringing it to an elevation that is only 0.7 feet from full, or 4098.6 feet. The reservoir outflows eventually enter the Belle Fourche River watershed. The chief of facility operation and maintenance and engineering services for Reclamation's Dakotas Area Office said, "Inflows since Oct. 1, 2011 (water year 2012) were 143 percent of average." When the reservoir becomes full, a small amount of water will flow out of the uncontrolled spillway of the dam and a small controlled release from the outlet works will begin at 50 cubic feet per second. The Belle Fourche Reservoir is currently at elevation 2970.15; full reservoir elevation is 2975.0. At the end of February, the diversion dam river outlet gates began diverting Belle Fourche River flows to Inlet Canal which flows into the Belle Fourche Reservoir. Additional inflows from Owl Creek, which flows directly into the reservoir, also contribute to the reservoir during snow melt and precipitation events. Source: http://rapidcityjournal.com/news/local/communities/belle_fourche/keyhole-reservoir-high-belle-fourche-near-full/article_42846d24-6c94-11e1-8d04-0019bb2963f4.html

NATIONAL

Corps: Don't get complacent. Officials from the U.S. Army Corps of Engineers met March 15 with the governor in South Dakota's state capitol to update him on the status of the Corps' post-flood damage studies and dam and structure repairs. The Corps is leading a delegation of engineers and others touring the river's six big dams from Montana to Nebraska the week of March 12 as the Corps moves on from completed critical levee and dam repairs to launching an

UNCLASSIFIED

UNCLASSIFIED

estimated \$186.3 million in continued work. South Dakota's governor pressed Corps officials to develop a more comprehensive method of determining the amount of snow in the northern Plains and its likely impact on spring runoff into the reservoir system and, eventually, downstream past Omaha and beyond. Source:

<http://www.omaha.com/article/20120315/NEWS01/703159914#corps-don-t-get-complacent>

FBI agent: Midwest militia group had 'kill' list. A midwestern militia group whose members are accused of plotting to murder police had a "kill list" that included current and former U.S. presidents, top government officials, and members of Congress, an FBI agent testified March 13 in a Detroit federal court. The list from members of the group called the Hutaree was titled "Established Elite Still in Control" and included military officers, reporters, and corporate executives, the FBI agent said. The agent, who had gained access to the group by posing as a truck driver, said the list was circulated during the wedding of a Hutaree leader. Seven members of the Hutaree face federal charges of sedition, the attempted use of weapons of mass destruction, and firearms offenses. Defense attorneys argued the group was merely engaging in angry expressions of free speech and did not intend to commit acts of terrorism. The trial is the latest in prosecutions aimed at what the government sees as a growing threat of violence from home-grown anti-government groups. Source:

http://www.msnbc.msn.com/id/46722890/ns/us_news-crime_and_courts/#.T2H4ZnkehBm

INTERNATIONAL

Iran cut off from global financial system. Dozens of Iranian banks were blocked from doing business with much of the world as the West tightens the financial screws on the country. The Belgium-based company that facilitates most international bank transfers took the unprecedented step March 15 of blocking 30 Iranian banks from using its service. The move is likely to hurt Iran's all-important oil industry and make it difficult for citizens to receive money from relatives living abroad. The move by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is part of a broader effort by Western nations to isolate Iran financially and force it to demonstrate it is not trying to develop nuclear weapons. The SWIFT said it was forced by recent European Union sanctions to discontinue service to Iranian banks beginning March 17. The SWIFT is a secure private network used by nearly every bank around the world to send payment messages that lead to the transfer of money across international borders. Source: <http://www.kansascity.com/2012/03/15/3492507/swift-financial-service-cuts-ties.html>

BANKING AND FINANCE INDUSTRY

Remote-controlled Android malware stealing banking credentials. Security researchers at McAfee have discovered a malicious Android application capable of grabbing banking passwords from a mobile device without infecting the user's computer. The latest piece of Android Malware, dubbed FakeToken, contains man-in-the-middle functionality to hijack two-factor authentication tokens and can be remotely controlled to grab the initial banking password directly from the infected mobile device. The malicious application targets specific

UNCLASSIFIED

UNCLASSIFIED

well-known financial entities posing as a Token Generator application. When the application executes, it shows a Web view component that displays an HTML/JavaScript Web page that pretends to be a Token Generator. The page also appears to be from the targeted bank. To get the fake token, a researcher discovered the user must enter the first factor of authentication. “When the user clicks ‘Generate,’ the malware shows the fake token (which is in fact a random number) and sends the password to a specific cell phone number along with the device identifiers (IMEI and IMSI). The same information is also sent to one of the control servers along with further data such as the phone number of the device. The malware finds the list of control servers from an XML file inside the original APK,” he added. He said the malware also contains commands to update itself or spy on the infected machine. The researcher found the FakeToken app can also hijack the list of contacts stored in the device (name and number). Source: <http://www.zdnet.com/blog/security/remote-controlled-android-malware-stealing-banking-credentials/10804>

Cybercriminals bypass e-banking protections with fraudulent SIM cards, says Trusteer.

Cybercriminals are impersonating victims to obtain replacement SIM cards from mobile carriers, which they then use to defeat phone-based Internet banking protections, security vendor Trusteer said in a March 13 blog post. Trusteer researchers have recently seen variants of the Gozi online banking trojan injecting rogue Web forms into online banking sessions to trick victims into exposing their phone’s international mobile equipment identity number, in addition to other personal and security data. The likely explanation for the collection of phone-specific data is it is used to obtain a fraudulent SIM card for the phone number by reporting the phone as stolen, Trusteer’s director of product marketing said. This would allow fraudsters to bypass bank anti-fraud defenses based on one-time passwords (OTPs). OTPs are unique codes online banking customers receive on their phones when money transfers are initiated from their accounts. These codes need to be inputted into the bank’s Web site to authorize those transactions. Fraudsters have developed several techniques to defeat such anti-fraud systems. Impersonating victims to obtain fraudulent SIM cards is a new method that serves the same purpose. Source: http://www.pcworld.com/businesscenter/article/251741/cybercriminals_bypass_ebanking_protections_with_fraudulent_sim_cards_says_trusteer.html

JPMorgan paying \$45 million to settle mortgage suit. JPMorgan Chase & Co. is paying the federal government \$45 million to settle a lawsuit alleging it charged veterans hidden fees in mortgage refinancing, according to court documents filed March 12. The whistleblower lawsuit, filed in 2006 in Georgia, seeks payments on behalf of the U.S. government by eight banks and mortgage companies, a law firm involved in the case said March 13. JPMorgan is the first bank to reach a settlement. According to court documents, the payment was part of the national mortgage settlement over foreclosure abuses reached with JPMorgan and four other lenders in February. The case is still pending against the other lenders, including Bank of America Corp, Wells Fargo & Co, and Citigroup Inc. Source: <http://www.reuters.com/article/2012/03/13/us-jpmorgan-settlement-idUSBRE82C0R220120313>

UNCLASSIFIED

UNCLASSIFIED

Fraud to hit more than 1,000 cardholders. After all is said and done, there will be more than 1,000 debit/credit cardholders in the southeast Iowa region, particularly in the Burlington area, who will have been affected by a recent wave of fraudulent transactions that surfaced in recent weeks, the Burlington Hawk Eye reported March 10. That figure is estimated based on the current number of customers area banks said have been victimized or have the potential of their card data being illicitly used. The transactions reportedly have occurred at retail stores from California, the East Coast, and as far north as Canada. Local law enforcement and bank fraud detection units are working to pinpoint the common denominator for the breach. Also, there have been reports of many cell phone customers having received a text message about their debit cards. The message indicates there is a problem and to call the number provided. "We're thinking of reissuing somewhere in the neighborhood of 400 cards," the president of Two Rivers Bank & Trust said. Officials at First Federal Bank proactively approached the problem, according to its president. "It's about 400 customers in southeast Iowa," he said. First Federal got information the past 2 weeks from Shazam, a card services company, about the cards and how many were affected by fraudulent transactions. Source:

<http://www.thehawkeye.com/story/Fraud-031012>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Key nuclear plant safety order likely to be delayed, NRC tells Senate. The Nuclear Regulatory Commission (NRC) will likely fall behind schedule in issuing a key safety measure designed for U.S. nuclear power plants, the agency's chairman told a Senate committee March 15. The NRC's five commissioners testified before the Senate's Environment and Public Works Committee on the safety progress of the U.S. nuclear industry a year after an earthquake caused a nuclear disaster at Japan's Fukushima Daiichi plant. The NRC chairman said U.S. nuclear power plants would likely miss the agency's 5-year goal for implementing orders aimed at avoiding the effects of earthquakes on the plants. An agency task force on the Japanese disaster said the measures should be put in place at the nation's 104 nuclear power plants by 2016. But the chairman said the earliest completion date for key seismic upgrades at the plants would be in 2017, and 2019 for low-risk plants. Source: http://www.washingtonpost.com/blogs/federal-eye/post/key-nuclear-plant-safety-order-likely-to-be-delayed-nrc-tells-senate/2012/03/15/gIQAX5maES_blog.html

Hospital audit finds radioactive materials unsecured. Congressional auditors found many hospitals with lax or improper security of medical radioactive materials, the New York Times reported March 14. In testimony prepared for delivery to a Senate panel, a Government Accountability Office (GAO) official planned to say that people with responsibility for security told the auditors that they were trained as physicists or radiation health technicians and were being told to enforce rules "that they did not believe they were fully qualified to interpret." The materials, such as cesium 137, could be included in a device with conventional explosives to make a "dirty bomb." There are about 1,500 hospitals and medical buildings that use radioactive materials, according to the Energy Department, which has spent about \$96 million to secure them. Source: <http://www.nytimes.com/2012/03/14/us/hospital-audit-finds-radioactive-materials-unsecured.html? r=1>

UNCLASSIFIED

UNCLASSIFIED

New NRC rules aimed at preventing explosions. The U.S. Nuclear Regulatory Commission issued two “Fukushima-related” orders to all nuclear plants in the country March 9. The first order “requires the plants to better protect safety equipment installed after the 9/11 terrorist attacks and to obtain sufficient equipment to support all reactors at a given site simultaneously.” The second order “requires the plants to install enhanced equipment for monitoring water levels in each plant’s spent fuel pool.” Other plants may be issued additional orders. Exelon Nuclear has until the end of 2016 to install a new ventilation system at the Limerick Generating Station in Limerick Township, Pennsylvania, designed to prevent the kind of explosions that blew apart Japan’s Fukushima Dai-ichi nuclear reactor buildings in March 2011. Source: <http://www.pottsmmerc.com/article/20120311/NEWS01/120319926/-1/BLOGS/new-nrc-rules-aimed-at-preventing-explosions>

COMMERCIAL FACILITIES

(Idaho) Meridian trailer park evacuated after bomb threat. Police said March 15 that they located what may be an explosive device that led to an evacuation of a trailer park near Meridian, Idaho. The Idaho Statesman reported that members of local bomb squads were working late March 14 to render the device safe. Authorities evacuated the Rose Circle Trailer Park, which has 30 to 40 homes, after they received information about a possible explosive device. Police also shut down two nearby intersections as part of the response. The FBI was assisting in the case. Source: <http://www.mansfieldnewsjournal.com/usatoday/article/38803343?odyssey=mod|newswell|text|Frontpage|s>

(New Jersey) Shooting at Woodbridge Center mall: Alleged shoplifter shot, killed by police; customers run for cover. A suspected shoplifter who held a woman hostage at knifepoint inside Woodbridge Center in Woodbridge, New Jersey, was shot to death by a police officer March 8, authorities said. After the man was confronted by mall security for an alleged shoplifting, the suspect put a knife to the throat of a random shopper and pulled her inside another store. An off-duty Woodbridge police officer who was wearing his police uniform and working an extra duty job at the mall shot the suspect after repeated warnings, killing him. Source: http://www.nj.com/news/index.ssf/2012/03/shooting_at_woodbridge_center.html#incart_mce

COMMUNICATIONS SECTOR

(New York) Thieves try to take copper from Falls cell tower. Two men attempting to steal copper wiring and metal piping from a cell phone tower and generator in Niagara Falls, New York, were interrupted when a technician arrived to determine why power had been cut. Police were called to a warehouse March 9, and were met by a field operations technician for Cricket Communications. The worker said Cricket has a cell tower and generator on top of the warehouse along with copper wiring running behind the building. The technician said he received a call from the network operator informing him power had been lost. When he

UNCLASSIFIED

UNCLASSIFIED

arrived, he heard someone running and tried to chase the suspects down but was unsuccessful. He then found copper wiring from the tower and generator had been removed and rolled onto spools, and metal piping had been cut and placed on the ground. Police found a pair of bolt cutters nearby. The owner of the warehouse looked at surveillance video and said the footage shows two people with flashlights near the phone generator rolling up copper wiring. Damage to the tower and generator was estimated at \$5,000. Source: <http://niagara-gazette.com/local/x2029123084/Thieves-try-to-take-copper-from-Falls-cell-tower>

CRITICAL MANUFACTURING

FAA proposes wiring change on Boeing 737. The U.S. Federal Aviation Administration (FAA) proposed changes on the overhead panel and wiring for Next Generation Boeing 737 aircraft, Fly Away Simulation reported March 15. This follows reports that three pilots failed to manually activate air data sensor heating systems on the aircraft as part of a pre-takeoff checklist procedure. "The affected airplanes do not have an automatic activation of the air data sensor heating system," said the FAA. "Pilots activate the system manually as a pre-takeoff checklist item. Failure to activate the air data sensor hearing system could result in ice formation on air data system sensors, which could lead to misleading airspeed data or loss of all airspeed indicating systems, and loss of control of the airplane." According to FAA estimates, these changes would take 80 hours per aircraft to implement, and will cost about \$15 million for the 1,025 Boeing aircraft in the U.S.-registered fleet. These changes would need to be implemented within 2 years. Source: <http://flyawaysimulation.com/news/4392/faa-proposes-wiring-change-on-boeing-737/>

NHTSA recall notice - Subaru Forester seat belt assemblies. Subaru announced March 15 the recall of 275,000 model year 2009-2012 Forester vehicles manufactured from November 26, 2007 through March 13. The automatic locking retractor in the seat belt assemblies located in the rear center seating of the affected vehicles do not meet lockability requirements and fail to comply with federal motor vehicle safety standards. Specifically, the assemblies may not permit proper installation and secure attachment of a child restraint in that seating position. An insecure installation of a child restraint can increase the risk of injury to a child during a crash. Subaru will notify owners, and dealers will replace the rear center seat belt assembly with a newly modified automatic locking retractor. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V099000&summary=true&prod_id=409764&PrintVersion=YES

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Tens of thousands of emergency responders nationwide get training in HAZMAT program. The American Chemistry Council trained 60,000 emergency responders nationwide in safety

UNCLASSIFIED

UNCLASSIFIED

techniques for a common, yet possibly highly-dangerous chemical, Government Security News reported March 14. The council said through its Transportation Community Awareness and Emergency Response (TRANSCAER) program thousands of emergency responders across 37 states received training in the safe handling and distribution of anhydrous ammonia, a common chemical used in agricultural and refrigeration industries. TRANSCAER, it said, is a voluntary national outreach effort that helps communities prepare for and respond to possible hazardous material transportation incidents. Program members consist of volunteer representatives from the chemical manufacturing, transportation, distributor, and emergency response industries, as well as the government. The Anhydrous Ammonia Training Tour initiative, said the association, is the first nationwide, product-specific training module of its kind. Launched in the spring of 2011, the program concentrates on a number of topics, including ammonia properties, transportation protocol, equipment handling, and emergency response in the event of a release, it said. The tour focuses on regions of the country where the use of anhydrous ammonia in agriculture and refrigeration applications is prevalent, it added. Source: http://www.gsnmagazine.com/node/25838?c=law_enforcement_first_responders

(Pennsylvania) Two 911 emergency dispatch outages blamed on Verizon. Westmoreland County, Pennsylvania officials said they hope the third disruption of service to the 9-1-1 dispatch system will be the last. The system sustained sporadic outages March 11, prompting dispatchers to use portable radios for about 15 minutes to send emergency-response crews to the western part of the county. The outage was the third in the last 2 weeks at the emergency dispatch center in Hempfield. The commissioners said March 13 a review of operations determined a glitch that affected communications March 11 and March 8 was caused by equipment provided by Verizon — not related to internal software and other county computer system failures. A Verizon spokesman confirmed March 13 investigators determined the outages were caused by a failed telecommunications computer card that works with the radio-dispatch system. The card was changed March 12. A public safety department spokesman said the latest outage affected only dispatches. No 9-1-1 calls were lost as a result of the malfunction. Source: http://www.pittsburghlive.com/x/pittsburghtrib/news/westmoreland/s_786392.html

GAO: New emergency responder network lacks critical features. A recent Government Accountability Office (GAO) report concluded limitations in the government's plans to create a nationwide broadband network for first responders will require the continued use of the existing system for at least another decade, Homeland Security Newswire reported March 12. The new broadband network will allow first responders from different jurisdictions to communicate, however, according to the GAO report, the new network lacks critical capabilities that the existing land mobile radio (LMR) systems have. As a result, existing LMR systems, which are expensive and limited in range, will continue to be used even after the new mobile broadband network is implemented. For instance the new network, with its designated Long Term Evolution standard, does not support basic voice capabilities such as push to talk, group talk, and talk around — features that first responders need. Without these features on the new mobile broadband network, the GAO report argued the existing LMR system must continue to

UNCLASSIFIED

UNCLASSIFIED

be used. Source: <http://www.homelandsecuritynewswire.com/dr20120311-gao-new-emergency-responder-network-lacks-critical-features>

ENERGY

(Ohio) Ohio: Gas-drilling injection well led to quakes. A dozen earthquakes in northeastern Ohio were almost certainly induced by injection of gas-drilling wastewater into the earth, state regulators said March 9 as they announced a series of tough new rules for drillers. Among the new regulations, well operators must submit more comprehensive geological data when requesting a drill site, and the chemical makeup of all drilling wastewater must be tracked electronically. The state department of natural resources announced the tough new brine injection rules because of the report's findings on the well in Youngstown, which it said were based on "a number of coincidental circumstances." They also noted the seismic activity was clustered around the well bore and reported a fault has since been identified in the Precambrian basement rock where water was being injected. Northeastern Ohio and large parts of adjacent states sit atop the Marcellus Shale geological formation, which contains vast reserves of natural gas that energy companies are rushing to drill using a process known as hydraulic fracturing. Source:

<http://online.wsj.com/article/AP6f04bbcf2fb9418d9a9befaa122c3dbd.html>

FOOD AND AGRICULTURE

Allergen alert: Cheetos with milk, soy. The Canadian Food Inspection Agency and PK Trading of Mississauga, Ontario, are warning people with allergies to milk or soy not to consume certain Frito Lay Cheetos because they contain milk and soy, which are not declared on the label, Food Safety News reported March 15. All codes of the following Frito Lay brand Cheetos products, imported from Korea, are affected by this alert: Cheetos (BBQ flavor, red bag) and Cheetos (Hot flavor, black bag). The recalled Cheetos were distributed in Ontario and Manitoba. Source:

<http://www.foodsafetynews.com/2012/03/allergen-alert-cheetos-with-milk-soy/>

CDC: Outbreaks linked to imported foods increasing. Foodborne illness outbreaks linked to imported food appeared to rise between 2009 and 2010, according to a new analysis released by the Centers for Disease Control and Prevention (CDC) March 14. The CDC reported half of the foods implicated in outbreaks were imported from "areas which previously had not been associated with outbreaks." The research was presented at the International Conference on Emerging Infectious Diseases in Atlanta. "It's too early to say if the recent numbers represent a trend, but CDC officials are analyzing information from 2011 and will continue to monitor for these outbreaks in the future," an epidemiologist in the CDC's Division of Foodborne, Waterborne, and Environmental Diseases and the lead author of the study said. The review found fish was the most common culprit, with 17 outbreaks total. The second most common food group was spices, with six outbreaks, including five from fresh or dried peppers. The CDC reported that nearly 45 percent of the foods tied to outbreaks came from Asia. Source:

<http://www.foodsafetynews.com/2012/03/cdc-outbreaks-linked-to-imported-foods-increasing-2/>

UNCLASSIFIED

UNCLASSIFIED

Allergen alert: Nuts in protein powder. Raw Elements Inc. is recalling Sunwarrior Warrior Blend Plant-Based Raw Protein because it contains tree nuts, an undeclared allergen, Food Safety News reported March 14. The raw protein was distributed in several Canadian provinces, including Alberta, British Columbia, Ontario, and Quebec. The recalled 1-kilogram raw protein has an enjoyed-best by date of March 2013. Source:

<http://www.foodsafetynews.com/2012/03/allergen-alert-nuts-in-protein-powder/>

Recall expands for beef linked to E. coli case. The February recall of certain beef burgers and beef steaks in Canada was expanded, according to the Canadian Food Inspection Agency, Food Safety News reported March 14. The beef may be contaminated with E. coli O157:H7 and has been linked to one illness. The expanded recall by New Food Classics of Burlington, Ontario is for: no name 12 Beef Burgers and no name Club Pack Beef Steakettes. These recalled burgers and steaks were distributed by Loblaw's nationally. Source:

<http://www.foodsafetynews.com/2012/03/canada-beef-recall-expanded/>

(New York) Wily, elusive foragers invade upstate New York. Feral pigs have been ransacking farms in upstate New York eating apples and other crops, the New York Times reported March 11. They roam by night, picking cornstalks clean, making off with apple crops. They have almost no natural predators, but they have razor-sharp tusks and a voracious appetite for plants and animals. Their population can triple in a year. Feral pigs have long plagued parts of the southern and western United States, now they have become a problem in the Champlain Valley of New York, an agricultural heartland on the edge of the Adirondacks. They hunt at night and steer clear of humans. The pigs devour ground-nesting birds and reptiles, fawns and domestic livestock, native vegetation, and crops. Wildlife managers and researchers nationally are exploring control measures, from contraceptives and poisons to snares and aerial shooting. Some are even employing night-vision equipment and thermal imaging. In New York, the state's ordinarily strict hunting rules have been relaxed for feral swine. The department of environmental conservation's Web site advises those with small game licenses to "shoot and keep feral swine at any time and in any number." Source:

<http://www.nytimes.com/2012/03/12/nyregion/feral-pigs-plaguing-upstate-new-york.html?smid=tw-nytmetro&seid=auto>

Allergen alert: Stew seasoning packaging error. McCormick & Company notified Publix Super Markets it is recalling a single lot code of Publix Beef Stew Seasoning Mix because it may have been packaged in error with brown gravy and may contain undeclared milk, Food Safety News reported March 13. The mislabeled beef stew mix was distributed in Alabama, Florida, Georgia, Tennessee, and South Carolina. Source: <http://www.foodsafetynews.com/2012/03/allergen-alert-beef-stew-seasoning-with-milk/>

U.S. scientists warn EPA on Monsanto corn rootworm. A group of U.S. plant scientists is warning federal regulators that action is needed to mitigate a growing problem with biotech corn that is losing its resistance to plant-damaging pests, Reuters reported March 9. The stakes are high — U.S. corn production is critical for food, animal feed, and ethanol production, and

UNCLASSIFIED

UNCLASSIFIED

farmers have increasingly been relying on corn that has been genetically modified to be toxic to corn rootworm pests. More than 20 academic corn experts sent a letter dated March 5 to the U.S. Environmental Protection Agency (EPA) telling regulators they are worried about long-term production prospects because of the failure of the genetic modifications in corn aimed at protection from rootworm. Monsanto introduced its corn-rootworm protected products, which contain a protein referred to as “Cry3Bb1,” in 2003 and they have proved popular with farmers around the country. Biotech corn sales are a key growth driver of sales at Monsanto. The product is supposed to reduce the need to put insecticides into the soil, essentially making the plants toxic to the worms that try to feed on their roots. However, plant scientists found evidence the genetic modification is losing its effectiveness, making the plants vulnerable to rootworm damage and significant production losses. The scientists said in their letter to EPA that the situation should be acted upon “carefully, but with a sense of some urgency.” Source: <http://www.reuters.com/article/2012/03/09/monsanto-corn-idUSL2E8E9ASB20120309>

Infant formula recalled due to ‘off odor’. Some Gerber Good Start Gentle powdered infant formula is being recalled, not because it poses a health or safety risk according to the Gerber Products Company, but because it might have an unpleasant odor, Food Safety News reported March 10. The company said it has received complaints that the product’s “off odor” has caused infants to spit up or have gastrointestinal issues. The recalled Gerber Good Start Gentle powdered infant formula is in a 23.2-ounce plastic package with an expiration date of March 5, 2013. Source: <http://www.foodsafetynews.com/2012/03/infant-formula-recalled-due-to-off-odor-1/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Ohio) 4 people injured in Ohio stabbing attack. Three people were in critical condition and one in stable condition after a stabbing incident March 14 in Columbus, Ohio, that ended with the suspect being shot by police, Columbus authorities said. The attack began inside a building that houses Miami-Jacobs Career College. The suspect was in critical condition at a hospital. A police official said a confrontation between two men in the admissions office led to one of the men stabbing the other. A witness in the office tried to intervene and also was stabbed, he said. The fight then spilled into the lobby, where the man stabbed two more victims, authorities said. The suspect was shot outside the building by an officer responding to the scene. The officer also used a stun gun to subdue the suspect. Three knives were recovered from the scene, one inside the admissions office, and two on the street where the suspect was shot, authorities said. A spokesperson for Miami-Jacobs Career College, said the campus was closed March 14 and March 15. Source: http://www.cnn.com/2012/03/14/justice/ohio-stabbing-attack/index.html?hpt=us_c2

(Texas) Woman shot dead outside courthouse. At least one person was shot dead by a man outside a county courthouse in Beaumont, Texas, local media reported March 14. An elderly woman was killed and at least three others were shot, including two rushed to the hospital with

UNCLASSIFIED

UNCLASSIFIED

several gunshot wounds, KFDM 6 Beaumont reported. The shootings took place outside the courthouse, in the basement of the county clerk's office, and at a bus station. The suspect reportedly surrendered to police after barricading himself in a building two blocks from the courthouse. A judge told KBMT 12 Beaumont the suspect is a man facing charges of having sexually assaulted his young daughter, who reportedly is mentally handicapped. He had been expected at a hearing the afternoon of March 14, the judge said. Source:

<http://usnews.msnbc.msn.com/news/2012/03/14/10686555-woman-reportedly-shot-dead-outside-courthouse>

Higher education breaches significantly down. In a year highlighted by the biggest data security breaches on record, colleges appear to have had a reprieve relative to prior years in terms of overall breaches reported and the corresponding number of total records breached, Help Net Security reported March 12. In 2011, there was a decrease in the total number of reported records affected (478,490), as well as institutions (48), that reported breaches. Both figures are all-time lows since data breach recording began in 2005, according to Application Security's TeamSHATTER. The largest reported data breach in 2011 by a U.S.-based institution of higher learning came from Virginia Commonwealth University (VCU), which reported a breach of 176,567 records in November. Other top victims included the University of Wisconsin Milwaukee (79,000), Yale University (43,000), and the University of South Carolina (31,000). VCU became the 21st higher education institution since 2005 to report a data breach in excess of 100,000 records and was the only one to eclipse that number in 2011. Three institutions exceeded the 100,000 mark in 2010. In 2005 – the first year reported data breaches were recorded – 6 higher education schools surpassed 100,000. According to the Ponemon Institute's most recent "Annual Study: U.S. Cost of a Data Breach" (March 2011), the findings showed the average cost to organizations per compromised record was \$214, though in the education vertical the average cost was far lower at \$112 per record. However, based on the lower education average, the VCU data breach could cost the university nearly \$20 million. Source: <http://www.net-security.org/secworld.php?id=12579>

Court hearing for man charged in threat letters. A Vancouver, Washington man charged in connection with threatening letters containing white powder that were sent to members of Congress and some media organizations agreed to be moved from a Washington state detention center to a Portland, Oregon jail, the Associated Press reported March 12. Once in Portland, he is expected to be arraigned on two criminal counts arising out of an investigation into the mailing of about 100 envelopes containing white powder. He was arrested March 9 in Washington state. The U.S. attorney's office said the letters, postmarked in Portland, so far have tested negative for toxic substances. Source:

http://seattletimes.nwsources.com/html/localnews/2017734404_aporcongressthreats.html

(Pennsylvania) Lancaster welfare office evacuated after white powder discovered. Authorities in Lancaster, Pennsylvania, said a state welfare office was evacuated after an employee opened a piece of mail containing a suspicious white powder, the Associated Press reported March 10. Emergency officials in Lancaster later determined the substance was not hazardous. About 200 people were ordered to leave the building for several hours March 9 while police investigated.

UNCLASSIFIED

UNCLASSIFIED

Lancaster police said six people exposed to the substance were taken to a hospital to be decontaminated and examined. Authorities said the powder was sent to a state police lab for further analysis. Source: <http://www.pottsmmerc.com/article/20120310/NEWS03/120319965/-1/OPINION01/lancaster-welfare-office-evacuated-after-white-powder-discovered>

(Maryland) UM student charged with threatening a ‘shooting rampage’. A student from Howard County threatened to go on a “shooting rampage” March 11 at the University of Maryland, College Park, campus police said. The student posted on a Web site comments such as “I will be on a shooting rampage tomorrow on campus”, “hopefully I kill enough people to make it to national news”, and “stay away from the Mall tomorrow at 1:30”, according to a release from university police. He was taken to a local hospital for an emergency psychiatric evaluation. He was unarmed when police apprehended him and charged with disturbing the orderly conduct of the activities, administration, or classes at the campus, a misdemeanor that could result in a \$2,500 fine or 6 months in jail. A department spokesman said police became aware of the threats March 10 after a former student noticed them on a Web site and two people who had contact with the suspect on another site informed the school; at least one was from out of state. The suspect was taken into custody on campus, near Cumberland Hall. March 11, the department spokesman said he was still at the hospital. University administrators suspended him, and he is no longer allowed on campus pending a review, police said. Source: <http://www.baltimoresun.com/news/breaking/bs-md-college-park-student-threats-20120311,0,1370540.story>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Digitally signed malware is increasingly prevalent, researchers say. Security companies recently identified multiple malware threats that use stolen digital certificates to sign their components in an attempt to avoid detection and bypass Windows defenses, IDG News Service reported March 15. When it was discovered in 2010, the Stuxnet industrial sabotage worm surprised the security industry with its use of rootkit components that were digitally signed with certificates stolen from semiconductor manufacturers Realtek and JMicron. Security experts predicted at the time that other malware creators would adopt the technique to bypass the driver signature enforcement in 64-bit versions of Windows Vista and 7. Given recent developments it appears they were right. A backdoor discovered by Symantec in December 2011 installed a rootkit driver signed with a digital certificate stolen from an undisclosed company. The certificate was revoked by VeriSign at the owner’s request 9 days later. However, the time window available for the malware to remain undetected was larger than that, because Windows operating systems rarely check certificate revocation lists, or do not check them at all, Symantec’s principal software engineer said March 15. Source: http://www.computerworld.com/s/article/9225237/Digitally_signed_malware_is_increasingly_prevalent_researchers_say?taxonomyId=17

Fake Google Play site serves Android malware. The recent name change of Google’s official Android Market — now called Google Play — has been recently taken advantage of by scammers, Help Net Security reported March 16. According to Trend Micro researchers, fake

UNCLASSIFIED

UNCLASSIFIED

Russian versions of the redesigned site have already appeared. “Download Google Play for Android Google Play is formerly known as the android market but now a vast and influential old android market combined with a store of books google ebookstore multi-format films and world music google music,” it is explained on the site. Among the suspicious Android apps offered for download is a Google Play application (google-play.apk), which is actually a Trojan that subscribes the victim to premium number services without asking his or her permission. The researchers said even if the Trojan in question is very similar to one discovered in February that has polymorphic abilities, this one does not, but tries to avoid detection by having various innocuous files added to it. Source: http://www.net-security.org/malware_news.php?id=2036

Malicious proxies may become standard fare. A number of security-as-a-service applications — from Postini to OpenDNS to Zscaler — reroute domain-name system (DNS) requests through centralized servers or proxies to detect security threats and sanitize traffic before it reaches the client network. Yet proxies are not just used by security companies, but by criminals as well. DNSChanger, which authorities shut down November 2011, used just such a strategy to reroute victims to custom advertisements and malicious installers. When the program compromised a system, it would replace the list of valid DNS servers with entries that pointed to servers controlled by the criminal operators, allowing the botnet owners to reroute victims’ Internet requests to any site. While DNSChanger itself did little damage with Internet traffic under the control of malicious actors, compromised systems quickly became laden with secondary infections. Source: <http://www.darkreading.com/advanced-threats/167901091/security/client-security/232602543/>

Fake online streaming service phishes and robs users. BitDefender researchers recently spotted a bogus online video player by the name of Web Player being offered to users searching for media players through Google. The player appears legitimate at first glance. During the installation process, it presents a EULA and information about its supposed developer, but once installed, it asks users to log in with an e-mail address and a password. Even though users do not have to share that data with the software to be able to “connect” to the video, it is probable many inexperienced ones do, thus allowing crooks to access their e-mail accounts. According to the researchers, no matter what data the victims type in, they are redirected towards an HTML page that allegedly offers a free-of-charge movie online player for many classic movies and new releases. The pages to which the users are taken change constantly, as they often get blocked by antivirus vendors. However, all require users to “register” with credit card data to watch the movies they want. As such, not only do the users get scammed to share their e-mail credentials, but also their credit card data. Source: http://www.net-security.org/malware_news.php?id=2033

Twitter being used by malware developers: Symantec. Symantec security researchers are seeing cyber criminals increasingly using Twitter as a way of luring mobile device users to their malware. In a March 12 post on Symantec’s blog, a company employee said tweets are becoming a popular way for cyber criminals to bring people to the Android.Opfake malware. “Users can potentially end up infecting their mobile devices with Android.Opfake by searching for tweets on subjects such as software, mobile devices, pornography or even dieting topics, to

UNCLASSIFIED

UNCLASSIFIED

name a few,” he wrote. “Android.Opfake is not hosted on the Android Market (Play Store) and these tweets lead to malicious Websites developed for the Opfake application.” These tweets, he said, usually have short URLs, and are primarily written in Russian, with some English mixed in. In addition, once the users get to the site, they are prompted to install the malicious code. However, while those are common aspects of most cyber criminals using Twitter, their individual tactics vary, making it difficult to determine which tweets are bad, short of actually clicking on the link. Source: <http://www.eweek.com/c/a/Security/Twitter-Being-Used-by-Malware-Developers-Symantec-770305/>

Google’s trap for Chrome exploit writers leads to crashes for users. A limitation built recently into Google Chrome to detect and block Flash Player exploits ended up breaking certain Flash-based applications and games for some users. Suspecting someone would try to hack Chrome via a Flash exploit at 2012’s Pwn2Own contest, the browser’s developers decided to restrict the maximum allowed size of Flash JIT (just-in-time) pages to a value that such exploits would likely exceed. The restriction was written in such a way that when the new limit would be reached the browser would throw an “access violation” exception that referenced memory address “0xABAD1DEA,” a hexadecimal value spelling out “a bad idea.” According to Chrome’s development tracker, the limit was introduced February 23 and was first tested out in the browser’s Canary (nightly build) version. The limit was later tweaked because of a considerable number of crash reports and landed in Chrome stable version 17.0.963.66 March 6. Source: http://www.computerworld.com/s/article/9225107/Google_39_s_trap_for_Chrome_exploit_writers_leads_to_crashes_for_users?taxonomyId=17

Pwn2Own ends with three browsers felled. By the end of the Pwn2Own competition at CanSecWest, Google Chrome, Microsoft Internet Explorer, and Mozilla Firefox were all subject to zero day exploits, the H Security reported March 12. Chrome fell a second time in Google’s own Pwnium contest with an attack that pulled together three zero-day vulnerabilities. The first Chrome exploit by the VUPEN team is thought to have leveraged flaws in the Flash player bundled with the browser, while their Internet Explorer exploit first provoked a buffer overflow on the heap working around DEP and ASLR protections. The team then made use of a memory error to break out of the sandbox (protected mode) of the browser. Mozilla Firefox fell to a team of two. Their zero day vulnerability in Firefox involved a use-after-free problem that evaded DEP and ASLR protections in Windows 7. According to reports, the vulnerability was used to leak data multiple times that was then used to prepare code to be executed, again through the same vulnerability. At Google’s Pwnium contest, Chrome fell a second time after a hacker going by the name of “Pinkie Pie” chained three zero-day vulnerabilities in Chrome together to break out of the sandbox and execute code. Google later patched Pinkie Pie’s vulnerabilities and announced the changes are being distributed in an update to the stable version of Chrome. Further changes are expected to harden the browser against CVE-2011-3046 and CVE-2011-3047, the CVE numbers allocated to Pinkie Pie’s vulnerabilities. Source: <http://www.h-online.com/security/news/item/Pwn2Own-ends-with-three-browsers-felled-Update-1469096.html>

UNCLASSIFIED

NATIONAL MONUMENTS AND ICONS

(Washington, D.C.) Washington Monument may be sinking, official says. The Washington Monument appears to be sinking, according to preliminary data collected by the National Geodetic Survey (NGS), CNN reported March 14. NGS surveyors and the National Park Service are investigating whether the August 23, 2011 earthquake in Washington, D.C., caused the 555-foot stone obelisk to sink or shift. “Our initial observations show a difference of around 2 millimeters at several of the survey markers in the vicinity of the monument,” said a chief geodetic surveyor. The monument was last surveyed in 2009. Since its completion in 1884, data shows it has sunk nearly 2 inches. The monument, the tallest structure in the nation’s capital, has been closed since the magnitude 5.8 quake struck. The earthquake may be responsible for the monument to have sunk 1 millimeter, while the other millimeter may be a result of normal settling, according to the surveyor. NGS is expanding the scope of its study to determine whether other national monuments are slipping back into the swampland upon which the nation’s capital was built. Source: http://www.cnn.com/2012/03/14/us/washington-monument/?hpt=tr_c2

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

Drug data reveal sneaky side effects. An algorithm designed by U.S. scientists to trawl through a plethora of drug interactions has yielded thousands of previously unknown side effects caused by taking drugs in combination. The work, published March 14 in Science Translational Medicine, provides a way to sort through the hundreds of thousands of “adverse events” reported to the Food and Drug Administration (FDA) each year. The team compiled a database of 1,332 drugs and possible side effects not listed on the labels for those drugs. On average, the program found 329 side effects for every drug, when most drug labels list an average of 69 effects. The new program, developed at Stanford University, combs through millions of doctor and patient reports to the FDA, Canada’s MedEffect, and similar databases. Source: <http://www.nature.com/news/drug-data-reveal-sneaky-side-effects-1.10220>

Thieves stealing old X-rays nationwide. A report filed with Huntsville, Alabama police said two 55-gallon barrels containing up to 1,000 patient information microfilms (X-rays) were stolen from Huntsville Hospital March 7. But the crime was not about identity theft. Instead, hospital officials think the thieves plan to melt the X-rays to extract the silver in them, as the films did not contain sensitive medical records. The stolen X-rays could be worth up to \$1,200 in extracted silver, said the director of sales for a New Hampshire medical recycling firm. Huntsville Hospital’s biggest concern about the episode may be the security breach that allowed someone posing as a vendor to come into the hospital and take away the barrels. The barrels were waiting to be collected by a vendor. Other recent cases include a Toronto, Canada, man who was charged with fraud in Ottawa after nearly 30,000 X-rays were stolen from

UNCLASSIFIED

hospitals and clinics across Ontario province. And the Lowell Sun of Lowell, Massachusetts reported the week of March 5 that two Florida men were charged with stealing a 50-pound barrel of used X-rays from Lowell General Hospital. Source:

<http://www.myfoxdfw.com/dpp/news/national/Thieves-Stealing-Old-X-Rays-Nationwide-031512>

TRICARE customers report fraudulent transactions. Nextgov reported March 15 that some of the 4.9 million individuals whose sensitive information was found on TRICARE tapes from a data breach in 2011 are reporting unauthorized transactions being made from their bank accounts. Currently, there are eight separate lawsuits filed over the TRICARE data breach demanding \$4.9 billion from the Department of Defense. A complaint amended to one lawsuit revealed many plaintiffs had to cancel their credit cards and close their bank accounts after they noticed that their assets were compromised. Therefore, it is now believed that the theft was targeted; the car the tapes were stolen from was a compact model surrounded by a number of luxury cars, all of which remained untouched. "The thief or thieves stealthily broke into the employee's Honda Civic and took the unencrypted backup tapes and records, thereby gaining information worth billions of dollars. The nature of this theft supports the logical inference that the thief or thieves were specifically targeting the confidential information contained on the backup tapes and records," the complaint reads. Source: <http://news.softpedia.com/news/TRICARE-Customers-Report-Fraudulent-Transactions-258830.shtml>

Nationwide drug shortage problem increasing. A nationwide drug shortage that is dogging the Food and Drug Administration (FDA) is hitting home with first responders CNN and WCBS 2 New York reported March 10. For emergency medical technicians, shortages can mean the difference between life and death. Nationwide, anti-seizure drugs including intravenous Valium, Versed, and Ativan are among the dozens of drugs — including cancer treatments — that are in short supply. The Monmouth Ocean Hospital Service Corporation Health Services ambulance service said it had to special order a temporary replacement anti-seizure drug to avoid running out the weekend of March 10. The FDA said it tracked at least 220 shortages in 2011, and claims it prevented 114, but admits the problem is far from solved. Source: <http://www.wdam.com/story/17126976/nationwide-drug-shortage-problem-increasing>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

(California) Report: Calif. nitrate contamination spreading. A study, ordered by the California legislature, shows chemical fertilizers and livestock manure are the main source of nitrate contamination in groundwater for more than 1 million Californians in the Salinas Valley and parts of the Central Valley. According to the University of California, Davis study released March 13, nitrate contamination of drinking water is a pervasive problem in California's agricultural heartland and is bound to intensify in coming years. The study concluded half of the 2.6 million

UNCLASSIFIED

UNCLASSIFIED

people in those areas live in communities where raw drinking water sources have registered nitrate levels exceeding the standard. Many of those communities blend or treat their water, drill a new well, or provide another alternative source, passing on extra costs to rate payers. The study offers an assessment of how many people are exposed and identifies solutions and costs. The study also found that about 1 in 10 people in the area rely on untreated groundwater that may exceed nitrate standards. If nothing is done, the study concludes, the financial burden on many agricultural communities could increase. By 2050, nearly 80 percent of the population — about 2 million residents — in the study area could have nitrate contamination exceeding the state standard. The study claims cleaning up polluted aquifers would be too difficult, and says improved farming practices and water blending, treatment, and alternative water sources are more cost effective. Addressing current nitrate contamination will potentially cost the state \$20 million to \$35 million per year. The study proposes a fertilizer tax that would be used by affected communities to mitigate for nitrate contamination. Another funding option is water use fees from affected residents. The study found nitrate leaching from agricultural land is responsible for 96 percent of current groundwater contamination. And while fertilizer use has leveled off in recent years, the amount of dairy manure has increased, making for a net increase over the past decade in nitrates loaded into the ground. Source:

http://www.boston.com/news/nation/articles/2012/03/13/report_calif_nitrate_contamination_spreading/

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center**: 866-885-8295 (IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio**: 800-472-2121; **Bureau of Criminal Investigation (BCI)**: 701-328-5500; **North Dakota Highway Patrol**: 701-328-2455; **US Attorney's Office Intel Analyst**: 701-297-7400; **Bismarck FBI**: 701-223-4875; **Fargo FBI**: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED